FDATA Feedback to FCA Consultation Paper 18/25

Primarily concerned with guidance for firms relating to PSD2

12th October 2018

Table Of Contents

About FDATA

The Financial Data and Technology Association (FDATA) is a not-for-profit trade association of member firms that works in several markets. FDATA is exclusively focused on Open Banking and Open Finance related issues. FDATA Europe is one of the 'Chapters' of the association. More information about FDATA can be found at www.fdata.global

The views in this document and the linked feedback to the eighteen questions posed by the FCA's consultation paper are the views of FDATA Europe. FDATA Europe members offer a wide range of payment and new model financial services to millions of consumers and small businesses daily and provide innovative financial applications and services to empower customers to take fuller control of their financial lives. Most of FDATA membership have, until now, offered services powered by credential-sharing through to screen-scraping.

Our members are motivated to transition to the use of dedicated interfaces powered by APIs. This is predicated on the interactions with the dedicated interfaces being of equal or higher quality to screen-scraping, and supporting TPPs in carrying out their 'Basic and Necessary Functions' (Appendix 2).

Rationale

FDATA acknowledges that CP 18/25 is headed in the right direction, and aligned with the outcomes sought by FDATA members. We are encouraged by the FCA's engagement and flexibility to find solutions for the good of the PSD2 ecosystem.

FDATA Europe welcomes encouragement to ASPSPs to deliver PSD2 compliance to an acceptable standard through commitment to API specifications and conforming to standards such as those provided by the Open Banking Implementation Entity (OBIE). Our membership is concerned about a number of interconnected 'cliff edge' scenarios in PSD2 and the RTS, the EBA Guidelines and the FCA Approach Document. We view the remediation of these issues as essential to stimulating innovation and competition from Third Party Providers (TPPs).

Leading Statement

How can a TPP utilising screen-scraping continue as a viable service when the introduction of SCA on the ASPSP user interface inhibits this functionality completely, in the absence of a fit-for-purpose dedicated interface?

PSD2 at Article 97 mandates that when a PSU authenticates with an ASPSP to access their account, Strong Customer Authentication (SCA) must be applied. The framework for what constitutes SCA and its required elements, has been opined on by the EBA. As a result, it was made clear that the majority of ASPSPs in the UK (including the CMA9) are required to change their current authentication procedures.

The challenge for ASPSPs is to implement SCA on their customer portal in a way which satisfies regulatory requirements, whilst allowing TPPs continued access in the absence of the customer, also known as screen scraping. If an ASPSP decides to satisfy the possession element of SCA using PINsentry-generated codes, this code will change with every PSU login attempt. Due to the variance of the code with each SCA attempt, a screen-scraper is unable to store the PIN and use it for repeated logins. The same argument holds for all other possession elements, while it is not possible for TPPs to store and reuse inherence elements (e.g. FaceIds and FingerPrintIds).

The industry view is that SCA and screen scraping on one customer portal are mutually exclusive outcomes. If a position does not emerge which reconciles this issue, there is danger that screen-scraping services relied on by customers will be removed without warning, with no alternative available. Feedback from the major Identity Access Management product vendors (who cover 99% of ASPSP authentication services in the UK) is to the effect that they do not, both practically and theoretically, support the solution called for in the regulation.

The effect of this is catastrophic for any TPP who relies on screen-scraping for the continuity of their product or service. Many of the TPPs offer financial services which are tethered to the account access. Customer detriment on a mass scale would ensue, potentially impacting millions of customers.

At its least harmful, ceasing all screen-scraping will eliminate existing services customers use and enjoy. The only solution for TPPs whose viability relies on screen-scraping is to attempt to migrate to the dedicated interfaces. As it stands, ASPSP dedicated interfaces are not fit-for-purpose and as such migration has the potential to cause ruin for a number TPP businesses.

This being the case, the FCA must intervene and establish a framework to avoid customer detriment - leaving this to the market is an unacceptable risk.

At this point FDATA highlight comments made by the FCA in paragraph 17.79.

FDATA support this paragraph, and stress the importance of this provision shaping requirements on ASPSP practices. We recommend the FCA to go further to protect PSUs and TPPs by making the following statement:

‘An ASPSP must not implement an SCA-compliant authentication journey on any customer portal for six months after they receive an exemption.’

This will provision a time period in which TPPs can migrate their customer base to the dedicated interface. By omitting this, the FCA risk numerous businesses, and services relied upon by hundreds of thousands of PSUs across the UK. We believe this aligns to, and effectively supplements PSD2 Art.115, which requires ASPSPs not to implement measures which block or obstruct existing PISP / AISP services. This article is designed to protect existing business models, and the addition of the suggested clause builds on this to ensure that those businesses attempting to transition are given a grace period, during which they could also raised issues experienced with any ASPSP dedicated interface.

Following Statements

Further to the key issue raised in the leading statement, FDATA have two further fundamental concerns with CP 18/25 we purport is vital the FCA address.

Agreements between TPPs and ASPSPs

FDATA bring paragraphs 17.33, 17.73, 20.24, 20.45 to the attention of the FCA.

The clauses above have been contentious for TPPs across the ecosystem. FDATA does not believe the recommended solution to present a viable option for TPPs looking to use these platforms. Identity information (17.33, 20.24), account information frequency (17.73), control of SCA elements and continued access (20.45) are crucial for a TPP's ability to use an API platform for the purpose of competition and innovation, so to place them at control of ASPSPs contravenes the aims of PSD2, RTS (and the CMA Order).

The following scenario outlines the competition issue this creates:

A TPP offers a product which interacts with an ASPSP through its dedicated interface. At the TPP's inception, the ASPSP contracts with them to ensure elements of service which are (by virtue of the clauses referred to above) not available to other TPPs relying on the dedicated interface. As the TPP develops, the ASPSP may wish to withdraw the service and take over the space the TPP was occupying in the market. The ASPSP has the discretion to withdraw the agreement and prevent the TPP from doing business, and take over its market share.

To this, FDATA offer two solutions:

<u>Option 1</u>
Measures for TPPs to ensure PSUs intend continuing access, standardisation of agreements between ASPSPs and TPPs.

(a) The FCA amend statement 20.45 to reflect requirements of PSUs and TPPs.

This requirement should mandate that AISPs ensure a PSU intends for their account to be accessed on an ongoing basis. FDATA members share the view that there must be regular reassessments to review the PSU's consent at least every 90 days.To renew consent, the PSU must take some affirmative action.

The affirmative action to renew access need not satisfy SCA (because it does not offer any technical security advantage): a scenario may arise where an AISP provides a Personal Financial Management Product (PFM). A PSU has an account with the PFM and has given long lasting consent upon account registration. During the 90 day access period, the PSU logs into the PFM platform, and causes their data to be refreshed. This shows a clear intention to continue use of the product. As such, this affirmative action means access continues. Since PSD2 was drafted, much of the interaction with PFM has transitioned away from login to email, push notifications, SMS and potentially other methods of digital communication, which satisfy the demands of PSUs for receiving their financial information.

If the PSU does not take any action indicating an intention for continued access within the 90 days, such as logging in to the PFM platform, access stops.

The TPP is a regulated actor, and it would be straight forward for regulation to simply require that the TPP communicate with the PSU every ninety days confirming the access is maintained.

There is no industry expectation that ASPSPs grasp the wide range of products and services offered by TPPs. ASPSPs are not best placed to dictate requirements for continued access, and allowing this will result in discontent within the market. The added requirement of 90-day SCA is unprecedented and frustrating for PSUs, and serves to stifle how TPPs can compete can truly compete with ASPSPs.

Further detail on the thought process of the FDATA membership on re-authentication every 90 days is given in Appendix 5.

(b) The FCA should enforce measures relating to agreements between ASPSPs and TPPs.

FDATA strongly recommend that the FCA enforce more granular measures concerning agreements between TPPs and ASPSPs under 17.33, 17.73, 20.24 and 20.45. There must be standardisation for these agreements in both their terms and availability. An ASPSP must not be able to ‘pick and choose’ which TPP may innovate using PSD2.

Option 2
The FCA should enforce measures relating to agreements between ASPSPs and TPPs.

Other markets (such as the USA) have been trying to reverse out of the complexity caused by bilateral agreements between actors. FDATA strongly recommend that the FCA enforce more granular measures concerning agreements between TPPs and ASPSPs under 17.33, 20.24, 17.73 and 20.45. If there is to be agreements (which needs to be properly considered as setting a precedent which makes things unnecessarily complicated), there must be standardisation for these agreements in both their terms and availability. An ASPSP must not be able to ‘pick and choose’ which TPP may innovate using PSD2.

Exemption based upon Self-Attestation

FDATA raise the issue of self attestation. FDATA oppose views in CP 18/25 states that the responsibility for reporting of crucial functions of the PSD2 ecosystem should be placed on ASPSPs.

In FDATA's experience, self-attested statistics (such as Q25) present a clear issue of adverse incentives, and lead to response bias. The data collected is likely to be somewhat synthetic and misleading. FDATA is concerned that the levels of objectivity and transparency delivered by each ASPSP will be inconsistent..

Additionally, paragraph 17.146 states that all testing need not be complete at the time of the exemption request. FDATA highlight that this further impacts the validity of data by simply requiring ASPSPs to report vicariously on the views of the consumers of their APIs. This clearly leads to an opportunity for ASPSPs to omit negative feedback, creating what is likely to be an incomplete picture of their dedicated interface.

As such, FDATA propose that the FCA collect data from both TPPs and ASPSPs to demonstrate ASPSP conformance to performance targets. This approach has numerous benefits. Firstly, TPPs are uniquely positioned in the PSD2 ecosystem with the capability to provide direct insight to experience and success of the interfaces. Secondly, TPP data allows the FCA to cross-reference ASPSP data in order to reduce any potential for obfuscation. Further, it would also incentivise ASPSPs to report with maximum transparency in order to avoid conflict or discrepancy between data sets.

Ultimately, cross-referencing ASPSP statistics is likely to motivate ASPSPs to increase conformance, which will only lead increased market competition and positive customer outcomes.

It is essential that, for each organisation submitting an exemption request, third parties be given an opportunity to independently feedback directly to the FCA, as to the challenges they have faced interacting with any ASPSP, and the extent to which these have been resolved at the time of the exemption.

FDATA ask that the FCA make use of FDATA's feedback submission to the EBA Consultation Paper, attached. This submission offers a Proposed Exemption Criteria, outlining industry needs and clear ways to measure and monitor how ASPSPs deliver to meet those needs. A number of our responses contained here will reiterate feedback from our response to the EBA.

Responses to FCA CP 18/25 Questions

Question 1

Do you agree with our approach to assessing requests for exemption to the contingency mechanism and our related guidance? If not, please explain why.

Timeline for exemption

Based on FDATA's experience nine months after the initial PSD2 launch date, we are sceptical that by September 2019, UK ASPSPs (including members of the CMA9) will provide a workable dedicated interface that is of equal or higher quality to current screen-scraping services. As mentioned above, this is caveated with the requirement for SCA on the customer portals which could cause damage the fintech industry. FDATA reiterate the aforementioned points:

ASPSPs must impose SCA from the end of the transition period, meaning that screen-scraping becomes technically impossible without the customer present to authenticate every data request.

When ASPSPs implement SCA, should they get an exemption, the only viable option for TPPs will be to migrate to PSD2-dedicated interfaces.

The majority of current CMA9 dedicated interfaces are not yet fit-for-purpose. Given the package of recent measures introduced by OBIE, the CMA9 may provide a service of equivalence to screen-scraping in advance of the March - September 2019 deadlines, but it is not likely that the majority of ASPSPs will be able to reach the target.

The impact of implementing SCA with no viable alternative has the potential for far-reaching PSU and TPP detriment. One FDATA member TPP offers a money management service to 100,000 PSUs with Barclays accounts using screen-scraping and authentication with a memorable word. If Barclays replace memorable word as a factor of authentication to comply with SCA, then customers using the TPP will experience harm to their financial wellbeing, being unable to use the service they do today..

FDATA suggest that ASPSPs be required to have demonstrated three months of acceptable performance and availability without restricting screen-scraping capabilities through the implementation of SCA. This will assure TPPs that migration to the dedicated interface from screen-scraping will not negatively impact the continuity of their product or service. This will further allow TPPs three months to migrate screen-scraping services to Open Banking interfaces. The current timeline and exemption process means that they could have access via screen-scraping prevented, but in the absence of having seen and interacted with a complete, performant and stable dedicated interface as an alternative.

To facilitate this proposal, an ASPSP must deliver a live, dedicated interface meeting the market need and have received an exemption by 14th June 2019. If the FCA share the opinion that a number of high-profile ASPSPs will not be able to deliver a dedicated interface

that provides an equal to, or better than, service than screen-scraping, FDATA strongly recommend that the timelines for SCA be postponed.

ASPSP self-attestation as part of conformance testing and submission of exemption request

As discussed above, FDATA oppose views in CP 18/25 that state the responsibility for self-reporting of crucial functions of the PSD2 ecosystem should be placed on ASPSPs.

Firstly, we seek clarification from the FCA on whether data collected is in relation to testing activity or performance of the dedicated interface. Testing activity and performance of a dedicated interface have previously been treated as two distinct data sets by the EBA.

FDATA view any self-attested statistics (such as Q16 & Q25) as a clear issue of adverse incentives, leading to response bias. The data collected is likely to be somewhat synthetic and misleading.FDATA is concerned that the levels of objectivity and transparency delivered by each ASPSP will be inconsistent..

Paragraph 17.146 states that all testing need not be complete at the time of the exemption request. FDATA highlight that this means ASPSPs will be reporting vicariously on their own interfaces. Clearly this presents an opportunity to omit negative feedback, creating an incomplete picture of their dedicated interface.

FDATA therefore propose that the FCA collect data from both TPPs and ASPSPs to demonstrate ASPSP conformance to performance targets. This approach has numerous benefits. Firstly, TPPs are uniquely positioned in the PSD2 ecosystem with the capability to provide direct insight to experience and success of the interfaces. Secondly, TPP data allows the FCA to cross-reference ASPSP data in order to reduce any potential for obfuscation. Further, it would also incentivise ASPSPs to report with maximum transparency in order to avoid conflict or discrepancy between data sets.

Ultimately, cross-referencing ASPSP statistics is likely to motivate ASPSPs to increase conformance, which will only lead increased market competition and positive customer outcomes.

It is essential that, for each organisation submitting an exemption request, third parties be given an opportunity to independently feedback directly to the FCA, as to the challenges they have faced interacting with any ASPSP, and the extent to which these have been resolved at the time of the application for exemption.

FDATA ask that the FCA make use of FDATA's feedback submission to the EBA Consultation Paper, attached. This submission offers a Proposed Exemption Criteria (contained in Appendix 3), outlining industry needs and clear ways to measure and monitor how ASPSPs deliver to meet those needs. A number of our responses contained here will reiterate feedback from our response to the EBA.

Wide use

FDATA purport that Q22 and Q23 are not enough to provide evidence of wide usage.

The concept of widely used is opaque and ambiguous, and we refer back to comments made by FDATA to the EBA in the EBA consultation response:

'FDATA have omitted 'widely used' from our FDATA Proposed Exemption Criteria as we believe the term is too subjective. We believe that if an ASPSP's dedicated interface satisfies the seven FDATA Proposed Exemption Criteria points above it will become 'widely used' by TPPs. If an ASPSP's dedicated interface does not satisfy all seven proposed FDATA Proposed Exemption Criteria then it is not fit for purpose and will not become widely used by TPPs.

To reiterate, we believe an ASPSP's dedicated interface should only be considered widely used if and only if the dedicated interface satisfies all seven of our FDATA Proposed Exemption Criteria.'

ASPSPs self-attesting wide use of their dedicated interface will not provide a clear picture of whether the interface is widely used, subject to issues mentioned above. An exemption granted on the basis of a functioning test facility is nonsensical, the RTS requires a PSD2 interface to be 'widely used' and there is no possible interpretation of 'widely used' that allows for an interface not to be in the live market.

FDATA challenge whether the metrics the FCA have recommended on whether 'wide use' of an interface will provide meaningful insight. The number of TPPs and PSUs utilising an interface is not an absolute indicator of success. As such, FDATA proposes wording to the effect:

'The number of authorised TPPs that are offering screen-scraping in place of Open Banking dedicated interfaces.'

The FCA should obtain such data prior to the legal implementation of SCA. This will ensure that the interface is fit-for-purpose and at an acceptable standard for TPPs and PSUs to resume products and services as expected after SCA.

At Q23, guidelines state that the number of AISPs/PISPs/CPIIs using the interface can be used to indicate that an ASPSP has enabled use of an API interface for 3 months. This approach is not sufficiently granular. It provides no context as to the ease or success of use, the time period, or volumetric profile of use over said period. The FCA must be more specific, and require the ASPSP to provide references which can be drawn on to provide both qualitative and quantitative assessment, independent of the ASPSP itself.

At para 17.141, it appears that a mistake has been made. The RTS at Article 33(6) refers to the dedicated interface meeting particular conditions, one of which (at (b)) is having been designed and tested to the satisfaction of PSPs as defined in Article 30(5). It does not refer, as the CP suggests, to the point of judgement being the testing facility. This would be extremely difficult to use as the basis of any assessment, as the lack of connection to

banking settlement systems will preclude complete and representative functionality beyond the API layer.

At para 17.163 the CP refers to practical impossibility of providing evidence of wide usage, but with no clarification or what might constitute an acceptable problem in the justification of failing to provide such evidence. It appears that no evidence could be provided, without justification, and that reliance on availability of testing facilities (which may themselves not reflect the complete functionality of the live service) could suffice in place of the dedicated interface. This is a complete departure from the requirements of the RTS.

To highlight feedback given in relation to EBA guideline 2.1, making comparison between service levels for the resolution of issues with the interface used by an ASPSP's own channels and the dedicated interface available to TPPs is not analogous. Those using the dedicated interface will be accessing it as an application which provides a services to a potentially wide range of customers. Any problem with the dedicated interface could result in an interruption of service which would fundamentally impact the TPP business. Contrast this with an issue on an ASPSP's personal customer facing mobile application, where the primary business impact is to the ASPSP itself. In the absence of an ability to contract for Service Level Agreement between TPP and ASPSP (with consequent protection in the event of service interruption), it is essential that the service level for resolving problems be defined in a manner which enables adoption of the interface with a level of surety commensurate with running a business which depends on it.

As reflected in #1 above, there is clearly a need for some level of independent oversight when considering the resolution of problems affecting those using the dedicated interface. Q28 relies on ASPSPs assessing the severity of problems, the time of resolution, and the speed of resolution, when the primary impact of an issue is on a TPP, as opposed to the ASPSP itself. The ASPSP is disincentivised to report on itself in a critical manner, as this could result in an exemption being revoked. To expect an ASPSP to report that it is in breach of the conditions imposed by RTS Article 33(6)(a) and (d) is not going to drive trust and transparency in the marketplace.

Additionally in relation to Q28, the FCA will be aware that several of the ASPSPs in the UK have already implemented dedicated interfaces which are in use by a range of TPPs. Problems with these interfaces have already been raised (see https://github.com/openbankingspace/tpp-issues/issues), and as such there is no need to restrict the problems that must be reported on to those identified during testing activity. Live use (and problems raised during) should be considered, and evidence to the effect that their resolution has been prioritised should be made available.

Question 2

Do you agree with our proposal to require quarterly submission to us of the quarterly statistics ASPSPs are required to publish under the SCA-RTS? If not, please explain why.

FDATA agree that monitoring is a vital aspect of ensuring a consistent and competitive PSD2 ecosystem. For a number of our membership once migrated from screen-scraping to Open Banking interfaces, they will have no option but to continue using the dedicated interfaces. Therefore, FDATA agree that the FCA must have a primary role in the monitoring of the ecosystem.

The FCA will be unable to monitor the PSD2 ecosystem via quarterly statistics and here refer back to the FDATA response to the EBA consultation that provides the clear industry need for the PSD2 dedicated interface via Seven Proposed Exemption criteria (see Appendix 3).

The response also goes further to recommend ways in which a CA (e.g. the FCA) should monitor these criteria (see Appendix 4).

Question 3

Do you agree with our approach to receiving reports about problems with dedicated interfaces? If not, please explain why.

The FDATA membership disagree with this approach and have two separate concerns. Firstly, reporting solely to the FCA is not sufficient. This means that TPPs have numerous avenues to reporting problems with dedicated interfaces, namely; the FCA, OBIE, the respective ASPSP, and other TPPs.

As such, a centralised system must be made available and backed by the FCA. The system will allow TPPs to report problems that can be accessed by ASPSPs, TPPs, OBIE (or other standards body) and regulators. This will ensure that reported issues are transparent, correctly allocated and addressed. It should also be possible for reported issues to be shared across the market, otherwise (for example) every TPP integrating with an ASPSP would have to individually discover a service outage.

FDATA refer the FCA to systems that are already in place - https://github.com/openbankingspace/tpp-issues/issues.

At paragraphs 17.178-9, a problem has arisen with the API design offered by the OBIE. In that design, there are 7 API specifications for payment initiation functionality, 5 of which relate to future dated payments. In these designs, payment initiation is treated as an immediate activity, rather than approaching this as a long lived consent. The PISP must therefore initiate the payment as soon as consent has been given (and authentication taken place on the ASPSP platform), and the bank will then lodge a payment object which is executed at the future date.

The problem with this approach is that the PISP is blind to the availability of funds at the time of execution. Were the initiation to be treated in the context of a long lived consent, then this problem would not arise, as the PISP would not initiate the authenticated payment until the future date, at which point it could check whether funds were available and thus manage the execution risk referred to at para 17.177.

The consequence of the above is that any ASPSP implementing the OBIE standard will not be able to provide confirmation of the availability of funds at the point of execution for the majority of the payment resources available under the design.

Question 4

Do you agree with our changes to the Approach Document to reflect the EBA exemption guidelines, EBA Opinion and the SCA-RTS? If not, please explain why.

There are a number of issues the FDATA membership have with the current draft of the Consultation Paper, we raise the issues in turn.

Agreements between TPPs and ASPSPs

FDATA reiterate that paragraphs 17.33, 17.73, 20.24, 20.45 do not provide a viable solution to the frustration the related EBA clauses will bring to the ecosystem. The current drafting of the these paragraphs will bring with them a competition issue, in which a TPPs ability to innovate and compete is subject to an agreement with an ASPSP.

To this, FDATA offer two solutions:

Option 1:
(a) The FCA amend statement 20.45 to reflect requirements of PSUs and TPPs

This requirement should mandate that AISPs ensure a PSU intends for their account to be accessed on an ongoing basis. FDATA members share the view that there must be regular reassessments to review the PSU's consent at least every 90 days.To renew consent, the PSU must take some affirmative action.

The affirmative action to renew access need not satisfy SCA:
A scenario may arise where an AISP provides a Personal Financial Management Product (PFM). A PSU has an account with the PFM and has given long lasting consent upon account registration. During the 90 day access period, the PSU logs into the PFM platform, and causes their transaction data to be refreshed. This constitutes a clear intention to continue use of the product. As such, this affirmative action means access continues.

If the PSU does not take any action indicating an intention for continued access within the 90 days, such as logging in to the PFM platform, access stops.

There is no industry expectation that ASPSPs should grasp the range of products and services offered by TPPs. ASPSPs have limited insight into the circumstances dictating requirements for continued access, and allowing this will result in ASPSP implementations unlikely to meet the requirements of the TPP market, this being one of the principle requirements of the legislation. The added requirement of 90-day SCA is unprecedented and frustrating for PSUs, and additionally serves to stifle how TPPs can compete with ASPSPs.

(b) The FCA enforce measures relating to agreements between ASPSPs and TPPs

FDATA strongly recommend that the FCA enforce more granular measures concerning agreements between TPPs and ASPSPs under 17.33, 17.73 and 20.45. There must be standardisation for these agreements in both their terms and availability. An ASPSP must not be able to 'pick and choose' which TPP may innovate using PSD2.

Option 2:
The FCA enforce measures relating to agreements between ASPSPs and TPPs

FDATA strongly recommend that the FCA enforce more granular measures concerning agreements between TPPs and ASPSPs under 20.24, 17.33,17.73 and 20.45. There must be standardisation for these agreements in both their terms and availability. An ASPSP must not be able to 'pick and choose' which TPP may innovate using PSD2.

Account Holder Information

The FCA Approach Document stipulates that 'In line with the EBA Opinion, the information ASPSPs are required to provide or make available to a PISP or an AISP does not include information concerning the identity of the customer (for example, address, date of birth or national insurance number) as such information is not specifically required for the provision of PIS or AIS. However, the PSRs 2017 do not prohibit PISPs or AISPs and ASPSPs from agreeing to share such information (as long as data protection legislation is complied with)'. This means that ASPSPs are not obliged to provide PII to TPPs as these are not required for the provision of AIS or PIS.

However, our membership the opinion that **if Account Holder Information (e.g. the Account Holder Name) is not within the scope of data to be shared with AISPs and PISPs under PSD2, the dedicated interfaces are unworkable.** This is because if Account Holder information is not within the scope of data to be shared with AISPs and PISPs under PSD2 and the RTS on SCA and CSC, it is technically impossible for the TPP to know that any account or transaction data they pull from a dedicated interfaced is owned by their customer from whom they have obtained consent. This places them at risk of fraud and in breach of GDPR.

Banks in the UK have indicated that they will not provide account holder information through the dedicated interface. As a consequence, the competition objective of PSD2 will be harmed, as ASPSPs seeking to enter the market as TPPs do not face this issue, given their ability to incept customers to their future services using identities they own. This immediately puts TPPs at a competitive disadvantage to ASPSPs .

An unseen circumstance is the creation of a market for unregulated screen-scraping of bank account holder information, this currently defined (in CP18-25) as beyond the scope of PSD2. The FDATA membership are aware of a number of unauthorised actors that are planning to continue screen-scraping Account Holder Information after the RTS comes into effect. This is because Account Holder Information now falls out of the scope of PSD2 and the RTS. This is not only antithetical to the objectives of the regulatory framework, but introduces significant risk to the market and adoption of Open Banking, as it results in unregulated handling of the most sensitive details of account information. This approach is off-putting to customers, and places them at the risk of negative outcomes if they do allow it to take place. Further detail is given within the response to the EBA consultation paper.

The Open Banking Implementation Entity, in their API design, have detailed an optional resource which serves information about account holders. If implemented, this would largely resolve the practical issue of a TPP being able to link the identity of the user of their service

to an account resource they can access as a result of a PSU authentication of a consent request. In this solution the TPP should ensure that existing provisions to obtain the PSU's consent are present in the user flow prior to authentication on the bank's platform, including consent to account holder information being shared.

The wider TPP community would not expect ASPSPs to be liable for the accuracy of this information beyond its connection to a particular account. For a range of business cases, TPPs are obliged to perform their own KYC checks and should still need to perform the same KYC checks after the account holder information is available through dedicated interfaces – the rationale for this service is to allow the TPP to link the identity of the PSU they interact with to a specific account.

Federation of Identity

From a technical point of view, the above solution introduces risk (due to the flow of personally identifiable information), and only partially addresses a broader problem, that of the decoupling of identities. At para 17.130 of CP18-25, it states "*In our view and in line with the EBA Opinion 33, where an interface allows for redirection, an AISP or PISP is not prevented from relying on the ASPSP issued credentials. This is because the AISP or PISP is able to 'use' the customer credentials and rely upon the ASPSP authentication procedures. Furthermore, the AISP or PISP is not required to issue its own credentials or authentication procedures*." **Both the EBA and FCA have misinterpreted the technical functioning of the redirect model in these opinions.** To form a relationship, any TPP must issue credentials to a user, to facilitate use and to enable them to be uniquely identified. In the most light-touch model, this would be through registration of email address and password. As authentication with the ASPSP is decoupled from the interaction with the TPP, it is technically impossible (in the redirect model) for the TPP to rely on the credentials used at the PSU-ASPSP interface to identify the customer. These credentials are never seen by the TPP.

CP18-25 foresees a solution at paragraph 20.24 – "*It is open to the ASPSP to allow a PISP, an AISP or another party to apply strong customer authentication on the ASPSP's behalf as part of a bilateral contract or arrangement. We would expect the parties to ensure that the contract addresses the allocation of liability between the parties.*" In technical terms, this would mean an ASPSP federating a digital identity service to a TPP, so that the PSU can log in to the TPP service using ASPSP-issued credentials (and attached digital identity) and the bank's authentication method. This is distinct from the redirect model as, since Strong Customer Authentication will have been applied at the outset, there is no requirement for a redirect. Additionally, there is no decoupling of identity, as the PSU uses only one at the point of inception.

The current drafting of the guidelines in the CP is problematic, as it leaves federation of identity to the discretion of the bank, and subject to a contract. This consequence of this is that banks have a discretion to offer a solution to TPPs of their choosing, or to leave others with the outstanding and problematic situation detailed above. If federated identity is to be dealt with in the scope of this legislation, it should not be left to chance and the discretion of

ASPSPs, as this has the potential to imbalance the playing field, against the environment of open innovation which the regulation seeks to create.

The FCA should consult with the EBA, taking advice from experts in digital identity, and redraft opinion 33 in terms which correctly reflect the technical working of the redirect model of customer authentication.

The FCA should consult with the EBA, taking advice from experts in digital identity, with a view to expanding para 20.24 to more strictly govern the federation of digital identity, and ideally commission a technical investigation into the creation of an industry-standard framework to homogenise this approach across the ecosystem. At the very least, should any ASPSP seek to offer enhanced SCA procedure or digital identity in the auspices of para 20.24, then this should be available to all TPPs on equal terms, costs and service levels.

Qualified Certificates

Within paragraph 17.147, the FCA comment on the use of Qualified Certificates. The FDATA membership ask the FCA qualify the obligations of ASPSPs in relation to the live use of Qualified Certificates, given that some of those FDATA members with PISP/AISP licences have obtained the certificates referenced.

Conformance Testing

FDATA members are in complete support for the comments made within paragraph 17.150. Our membership see these conformance tools providing a much more complete assessment of the Open Banking ecosystem.

Further Changes

In relation to paragraphs 17.24-25, it is asked that FCA comment on whether the scope of information should, in the case of a cross currency payment, include the rate information which is to be applied to conversion of one currency into another. This information is currently made available to customers directly, but there is strong indication from the major ASPSPs in the UK that they do not intend to deliver rate information to PISPs initiating payments which involve currency conversion. This would prevent the PISP informing the PSU of the cost of a proposed payment to a different currency, and consequently this would not form part of any consent between the PISP and PSU to initiate the payment.

It is the belief of the FDATA membership that this is essential, both in view of the FCA’s guidelines, and for the APIs which relate to this form of payment to be usable by PISPs. This is also of relevance given the wording of paragraph 17.35, which specifically calls out international payments. It is the belief of the FDATA membership that the customer should be able to initiate a payment via a PISP in full knowledge of the rate to be applied and consequent cost of the transaction, before they are redirected to authenticate, and that this information should not be retained by the ASPSP in its domain.

Question 5

Do you agree with our approach to receiving notifications relating to the fraud rate? If not, please explain why.

No comments.

Question 6

Do you agree with our proposed approach to the corporate payment exemption? If not, please explain why.

No comments.

Question 7

Do you agree with our proposed approach to the application of the strong customer authentication requirements and associated exemptions? If not, please explain why.

FDATA Europe does not agree with the current PSD2 and Regulatory Technical Standards (RTS) legal framework, the European Banking Authority (EBA) Guidelines and the FCA Approach Document. To protect payment service users (PSUs) and third party providers (TPPs) across the United Kingdom, it is essential for the FCA to review and remedy these issues as quickly as possible.

Issue: How can a TPP utilising screen-scraping continue as a viable service when the introduction of SCA on the ASPSP user interface inhibits this functionality completely, and does not offer an alternative fit-for-purpose PSD2 interface?

PSD2 at Article 97 mandates that when a PSU authenticates with an ASPSP to access their account, Strong Customer Authentication (SCA) must be applied. The framework for what constitutes SCA and its required elements, has been opined on by the EBA. As a result, it was made clear that the majority of ASPSPs in the UK (including all of the CMA9) will be required to change their current authentication procedures.

The challenge for ASPSPs is to implement SCA on their customer portal in a way which satisfies regulatory requirements, whilst allowing TPPs to continue to access this in the absence of the customer, also known as screen scraping. If an ASPSP decides to satisfy the possession element of SCA using PINsentry-generated codes, this code will change with every PSU login attempt. Due to the variance of the code with each SCA attempt, a screen-scraper is unable to store the PIN and use it for repeated logins. The same argument holds for one-time passcodes sent via SMS, while it is not possible for TPPs to store inherence elements (e.g. FaceIds and FingerPrintIds).

The prevailing industry view is that SCA and screen scraping on one customer portal are mutually exclusive outcomes. If a position does not emerge which reconciles this issue, there is danger that screen-scraping services relied on by customers will be removed without warning, with no alternative available.

The effect of this is catastrophic for any TPP who relies on screen-scraping for the continuity of their product or service. Material PSU detriment will ensue on a mass scale, affecting millions of customers.

At its least harmful, ceasing all screen-scraping will eliminate existing services customers use and enjoy. The only solution for TPPs whose viability relies on screen-scraping is to attempt to migrate to the Open Banking interfaces. As a fallback for such TPPs, the Open Banking interface is simply not fit-for-purpose and as such has the potential to cause ruin for a number of TPP businesses.

This being the case, the FCA must intervene and establish a framework to avoid customer detriment - leaving this to the market is an unacceptable risk.

The timelines for RTS were written before the evidence from the UK implementation on the size of the challenge was available.

Below is a revised timeline for PSD2 and RTS requirements that meets the market need, also contained in Appendix 1. Appendix 1 supplements this feedback with additional detail from FDATA's perspective concerning the current condition of the dedicated interfaces, and strategic considerations placed on ASPSPs by the current timeline.

Proposed revised timeline for exemption:

- Provide Testing and Specification by 14th March 2019 (no change)
- Make available a live production environment for 14th June 2019 (to give adequate time for the TPPs help the ASPSP.
- Apply for exemption by 14th September 2019
- FCA has three months of monitoring production until 14th December 2019
- ASPSP has three months to prepare an adjusted interface, until 14th March 2020.
- SCA requirement comes into effect 14th September 2020.

The market now needs radical intervention by regulatory authorities and policy makers to re-organised the timelines, reduce immediate risk and focus on the getting to the right answer.

Finally, FDATA would like to emphasise the importance of the FCA's ongoing review of exemptions. If a TPP migrates their services from screen scraping to a dedicated interface, it is essential that the dedicated interfaces continue to perform at the necessary and legal requirements. Migration back to screen scraping will, at best cause severe customer detriment and at worst be technically impossible.

Question 8

Do you agree with our approach to implementing the EBA fraud reporting guidelines? If not, please explain why.

No comments.

Question 9

Do you have any feedback on how the FCA can best use the data we would receive under the EBA fraud reporting guidelines?

No comments.

Question 10

Do you agree with our proposal to require PSPs and Credit Unions to record and report data on complaints they have received about alleged APP fraud in general? If not, please explain why.

No comments.

Question 11

Do you agree with our proposed Approach Document text clarifying our expectations in relation to PSPs' requirements where the wrong unique identifiers are used? If not, please explain why. 27 CP18/25 Annex 1 Financial Conduct Authority Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive (PSD2)

No comments.

Question 12

Do you agree with our proposed Approach Document text clarifying guidance in light of the contingent reimbursement code developments? If not, please explain why.

No comments.

Question 13

Do you agree with our other changes to the Approach Document? If not, please explain why. Please provide section references in your response.

No comments.

Question 14

Do you agree with our proposed changes to PERG regarding agents? If not, please explain why.

FDATA Europe is keen to see a market that protects customers and protects the ecosystem, whilst offering a the maximum level of flexibility to support diverse business models. We agree that the customer should know who is responsible for making them whole and should be able to easily identify who (in their service provision) holds their data and who is a regulated actor.

There is a diverse range of business models in the current market. It is clear that firms remain, despite the various attempts by the FCA to clarify the situation, unsure of range of their regulated position. Other firms were expecting to be regulated and have not been. It is reasonably clear that some firms that have not been regulated are performing similar market functions to some firms that are regulated, and that the provision of agents (offering the payment services of the principal in the short term) are effectively performing a 'regulated' Technical Service Provider service, as they are not the brand or service that the customer is engaging with.

It is crucial that there are no weak links in the chain of customer protection. Does the FCA scrutinise the contracts for AIS to ensure that other parties are able to assist in the liability model?

FDATA Europe hopes that the FCA will extend the consultation and hold a roundtable on this before firming up the CP. It is creating a challenging competitive environment and needs further attention.

Question 15

Do you agree with our proposed changes to PERG regarding e-commerce platforms? If not, please explain why.

No comments.

Question 16

Do you agree with our proposed changes to PERG regarding closed loop gift cards? If not, please explain why.

No comments.

Question 17

Do you agree with these changes to PERG? If not, please explain why.

No comments.

Question 18

Do you agree with the cost and benefits we have identified? If not, please explain why.

No comments.

Appendix

Appendix 1

The CMA9 were required by the CMA to put high quality, standardised APIs in the market on 13th January 2018, when PSD2 came into force.

The consultation period for FCA CP18/25 ends nine months after 13th January 2018, and yet many of the CMA9 are still not providing a quality that is acceptable to the market, hence the low adoption rate thus far. This is due to the significant and diverse range of continuing problems. The TPP market is reasonably confident that the CMA9 will not reach the required standard in time to be granted an exemption, whilst non-CMA9 ASPSPs will undoubtedly be in a position where an exemption application is not possible by September 2019. To put it in context, the CMA9, having started construction in January 2017 are going to find it very difficult to meet their PSD2 compliance requirements in time to be offered an exemption and the non-CMA9 will not receive an exemption by September 2019.

The FDATA membership has extensive experience in executing new technology and has been engaged throughout the PSD2 and Open Banking journey. The FCA may recall that it was the FDATA leadership that correctly called that the CMA9 were not going to be in a position to safely launch their read/write APIs in January in 2018 as far back as the August 2017. FDATA was then able to suggest a contingency plan which we negotiated directly with the CMA9 to request that the TPP market volunteer to throttle the number of real customers being pushed through the API, whilst the TPPs conducted market acceptance testing and the ASPSPs gained confidence in their security.

Based on our learning to date we are deeply sceptical of the proposed timeline. FDATA understands that the FCA has to somehow frame a timeline that aligns with PSD2 RTS and still reach market facing objectives. FDATA is of the strong opinion that these two objectives are now incompatible. The scenario below is one FDATA deem to be highly likely.

1. Some ASPSPs (primarily non CMA9) will recognise that it now not possible for them to get an exemption, because they have started too late and underestimated the requirements. They will focus on an adjusted interface model. This is a bad outcome for everyone who wants to see a progressive and innovative system.

2. The CMA9 will push hard to get to a point of getting an exemption by committing to a dedicated interface, delivered through a standard. To try to get there, they will go ‘all in’ without putting planning into the contingency measure.

3. According to the proposed timeline for an exemption, ASPSPs will have to have had their API delivery in the market for real customers by 14th March, so they can demonstrate three months of being ‘widely used’ prior to being tested in June. They

are required to release their specifications and testing facilities by the same date. This makes it impossible for the TPP to properly consume the API unless it is delivered to the OBIE specification and is (at the very least) full conformant to FAPI Security Profile. This would mitigate the testing facilities and specification provision timing issue.

4. If the TPP community has to connect to anything bespoke, we recommend that the FCA request that the ASPSP builds to the adjusted interface and does not offer exemption to any ASPSP that is not standardised. The TPPs will not have the bandwidth at this late stage to deliver bespoke integrations (based on the experience of even minor divergence from standards with the CMA9), and do not wish to see bespoke APIs in the market due to engineering time, risk and complexity of maintenance.

5. Even with this adjustment, FDATA believes the evidence shows that few ASPSPs will be fully stable and conformant for 14th June, if their first ‘release’ of software is in mid-March.

6. Based on our technical assessment of the requirements of the adjusted interface, it seems likely that the firms that have focused on preparing for testing and supporting their dedicated interface in support of their exemption application, will not then have sufficient time to also deliver an adjusted interface (which also requires a period of testing and integration) in time to satisfy TPP requirements and of meeting the standards of RTS.

7. The ability to utilise credential sharing through to screen scraping will cease with the SCA requirement that comes into effect on 14th September 2019. Without alternative stable alternatives that provide an equal or higher quality of service all TPPs utilising screen-scraping will be materially damaged.

8. The TPP market is aware that ASPSPs will have to comply with SCA-RTS requirement in respect of their direct customers, and could do so at any point between 12th October 2018 and September 14th 2019. It is likely that many will seek to phase this in prior to deadline. TPPs need to have some time of availability of either alternate channel (dedicated or adjusted interface) to transfer their customers from their current screen scraping channel.

9. The FCA needs to understand that if a firm (including any member of the CMA9) arbitrarily switches on universal SCA without concerted planning that the vast bulk of TPP customers will immediately be disconnect from their TPP. This would destroy the market and harm hundreds of thousands of PSUs financially.

10. FDATA therefore suggests that the FCA provides guidance that:

1. No ASPSP can switch on full SCA in their direct channel until 14th September and 3 months after the ASPSP is given the exemption or has provided a stable contingency measure.

2. That is no ASPSP is permitted to have SCA imposed in their direct channel, if the are not compliant with the dedicated interface or adjusted interface (contingency measure).

3. ASPSPs must turn off SCA, if at any point they fail to maintain the quality of their of the dedicated interface or adjusted interface.

4. ASPSPs signalling a commitment to building a standardised dedicated interface be given another six months to develop their compliant solution, whilst the above conditions are also in place. Therefore the requirement for SCA to be pushed back by

2. A revised timeline for exemption could be as follows:

- Provide Testing and Specification by 14th March 2019 (no change)
- Make available a live production environment for 14th June 2019 (to give adequate time for the TPPs help the ASPSP.
- Apply for exemption by 14th September 2019
- FCA has three months of monitoring production until 14th December 2019
- ASPSP has three months to prepare an adjusted interface, until 14th March 2020.
- SCA requirement comes into effect 14th September 2020.

The timelines for RTS were written before the evidence from the UK implementation on the size of the challenge was made available. It is clear that these are unworkable for most ASPSPs in the UK and across the EU.

The market now needs radical intervention by regulatory authorities and policy makers to re-organised the timeliness, reduce immediate risk and focus on the getting to the right answer, which is an orderly transition to.

Appendix 2

TPPs Must Be Able to Perform Basic and Necessary Functions

These functions are required of ASPSPs by established TPPs as well as TPPs that are new to the market, irrespective of business model. Our membership is of the opinion that these fundamental functions, at a bare minimum, **must** be supported by all ASPSPs in order for the PSD2 ecosystem to work.

The two basic and necessary functions required by TPPs are:

1. Collecting, de-duplicating and storing the account information/payment information provided by ASPSPs according to CA-mandated specifications; and
2. Linking the PSU who owns and authenticates the account information/payment information, to the PSU on the TPP interface, i.e. establishing the identity of the PSU.

If either of these two functions are not possible within both the legal framework and the technical delivery of ASPSPs, it will be impossible for the PSD2 market to function properly.

Appendix 3

FDATA Exemption Criteria:

- **The PSD2 dedicated interface is widely available**
  - The uptime of the PSD2 dedicated interface is greater than or equal to the ASPSP's private dedicated interface.

  Further detail is given in response to Question 1

- **The PSD2 dedicated interface is adequately responsive and maintains performance at scale**
  - The response time of the PSD2 dedicated interface is quicker than or equal to the performance of an ASPSP's private dedicated interface, at similar levels of stress; and
  - The PSD2 dedicated interface can endure similar levels of stress as the private interface can; and
  - If the PSD2 dedicated interface is unable to process TPP requests due to stress, consistent and conformant errors are provided to TPPs.

  Further detail is given in response to Question 2

- **The PSD2 dedicated interface is unobstructive**
  - PSUs adoption of the PSD2 dedicated interface is equivalent to or better than credential-sharing through to screen-scraping; and
  - The authentication journey conforms with the legislation; and
  - The PSD2 dedicated interface does not require TPPs and PSUs to be exposed to unnecessary obstacles.

  Further detail is given in response to Question 4

- **The PSD2 dedicated interface is conformant to the relevant specification.**

Further detail is given in response to Question 5

- **The account information/payment information data feed provided by the PSD2 dedicated interface is conformant, functional and complete**
  - The data feed the PSD2 dedicated interface provides to TPPs conforms to the legislated specification designed by the relevant CAs; and
  - The implementation of the account information/payment information data feed provided by the PSD2 dedicated interface allows TPPs to store the data provided without adding hindrance; and
  - The implementation of the account information/payment information data feed provided by the PSD2 dedicated interface allows TPPs to link the data provided to the respective PSU within the TPP's interface; and
  - The data feed the PSD2 dedicated interface provides to TPPs contains equivalent or more data than the data feed provided by the private interfaces.

  Further detail is given in response to Question 5

- **The PSD2 dedicated interface is appropriately managed**
  - Reported problems with PSD2 dedicated interfaces are addressed in a professional manner, similar to that shown to private dedicated interfaces; and
  - Appropriate notification is made available to TPPs in advance of any change made by an ASPSP where the change could cause an issue to the services a TPP provides to its customers.

  Further detail is given in response to Question 7.

- **The PSD2 dedicated interface is appropriately monitored providing confidence in stability**
  - An ASPSP provides evidence that their PSD2 dedicated interface has passed the above six criteria for the last three months.

  Further detail is given in response to Question 3.

Appendix 4

Recommendations for monitoring ASPSPs according to FDATA Proposed Exemption Criteria 1-6

The PSD2 dedicated interface is widely available:

- The CA benchmarks the PSD2 dedicated interface's availability against the private dedicated interfaces, providing a clear pass/fail.

The PSD2 dedicated interface is adequately responsive and maintains performance at scale:

- The CA benchmarks an ASPSP's PSD2 dedicated interfaces' response times to those of the ASPSP's private dedicated interfaces. If the response time of the PSD2 dedicated interface is significantly and consistently greater than the private dedicated interface then the PSD2 dedicated interface fails to perform at the necessary standard. This provides a clear pass/fail.
- The CA runs the PSD2 dedicated interface through the minimum stress level(s) (described further in response to question 2) if the dedicated interface remains responsive and conformant during the CA testing the dedicated interface passes this criterion. This provides a clear pass/fail.
- The CA in conjunction with the ASPSP overload the stress of the PSD2 dedicated interface. If the response to the stress overload are consistent and indicative of an overloaded system the dedicated interface passes this criterion. This provides a clear pass/fail.

The PSD2 dedicated interface is unobstructive:

- Where possible, CAs should engage with the TPP community in order to benchmark the sign-up rate of the PSD2 dedicated interfaces against the sign-up rate of credential-sharing through to screen-scraping. As these customer authentication journeys are like for like the the sign-up rate of credential-sharing through to screen-scraping provides a clear pass/fail. For the avoidance of doubt, customer sign-up rate via PSD2 dedicated interfaces should be greater than or equal to sign-up rate through credential-sharing through to screen-scraping.
- The CAs run the authentication journeys through a customer experience checklist to assess conformance, providing a clear pass/fail. Further detail on the customer experience checklist is given in response to question 4.
- The CAs analyse TPP complaints data and KPIs provided by the ASPSP and TPP to assess whether any unnecessary obstacles were created by the ASPSP.

The PSD2 dedicated interface is conformant to the relevant specification:

- The CAs make use of automated conformance testing suites to automatically test the dedicated interfaces' technical implementation, providing a clear pass/fail. Conformance testing should be run several times an hour as the results will provide insight into the PSD2 dedicated interfaces availability.

The account information/payment information data feed provided by the PSD2 dedicated interface is conformant, functional and complete:

- The CAs make use of automated conformance testing suites to regularly (several times an hour) test the dedicated interface account information/payment information data feed, providing a clear pass/fail.
- The CAs make use of automated conformance testing suites to provide clear indication of the content within the ASPSP's account information/payment information data feed. The CAs then assess whether TPPs can store the data without significant hindrance. When assessing this criteria CAs should be aware that the TPP may already have received and stored data feeds for a PSU with the similar content, i.e. the same fields provided. This criteria provides a clear pass/fail.
- The CAs make use of automated conformance testing suites to provide clear indication of the content within the ASPSP's account information/payment information data feed. The CAs then assess whether TPPs can reasonably link this data feed to the respective PSU on the TPP's interface. This criteria provides a clear pass/fail.
- The CAs benchmark the content of the ASPSP's account information/payment information data feed from the PSD2 dedicated interface against the content of data made available to the PSU via the ASPSP's PSU interfaces. If the content of the PSD2 dedicated interface's data feed is less than the content within the PSU interface's data feed, then the ASPSP should not be granted an exemption. This provides a clear pass/fail.

The PSD2 dedicated interface appropriately managed:

- The CAs engage with the TPP community where possible and analyse TPP complaints data as well as KPIs from ASPSPs and TPPs to assess whether any inappropriate management has occurred.
- The CAs provide a notification checklist that ASPSPs must conform to every time the ASPSP intends to make a change to the PSD2 dedicated interface that could result in a TPP requiring to make changes to their service. The notification checklist also notifies the relevant bodies of upcoming downtime, any changes to optional fields, . Further detail on the notification checklist is given in response to question 6.

Appendix 5

90 Day Re-authentication Issue

When PSD2 was drafted, it was assumed that the PSU would use their login credentials in the TPP domain to connect to the ASPSP. The SCA RTS requirement for 90 day re-authentication is of no security value. The reason for this, is that if an nefarious actor holds login credentials, they do have any impediment within a 90 day window. Given this requirement has nearly zero security value, it would appear that the main driver is to ensure that the PSU is aware they are still connecting their accounts to any TPP. A PSU may have many accounts connected to one TPP for a service.

Therefore the nuisance value alone, would see asymmetric competition afflict the TPP, who will suffer serious economic attrition my constantly losing access to their customers. By suffering unwitting or forgetful interruption of their service provision, the PSU will suffer materially risk. Financial services can be tethered to the access requirement and therefore the PSU could also be in breach of contract as well suffering loss of service or financial loss.